RGPD : Comment l'Europe s'apprête à débrancher son économie numérique

RGPD : le consommateur est le grand perdant des réglementations qui affectent le commerce. Quand bien même il serait prêt à faire de larges concessions sur ses données personnelles, on ne lui laisse plus le choix.

Par Ferghane Azihari.

L'entrée en vigueur du Règlement européen sur la protection des données personnelles a fait l'effet d'un couperet brutal à l'échelle internationale. Le magazine Forbes soulevait récemment que les coûts de conformité pour les entreprises américaines du classement Fortune 500 et les entreprises du FTSE 350 s'élevaient environ à 9 milliards de dollars. En réaction à la nouvelle réglementation, certains gros titres américains (Los Angeles Times, The Chicago Tribune, etc.) ont même renoncé à investir le marché européen.

Comble de l'incongruité, les internautes européens en sont réduits à adopter les mêmes méthodes que les populations vivant sous des régimes autoritaires pour accéder à certains sites étrangers en utilisant un VPN pour brouiller l'origine de leur connexion. En cause, les incertitudes juridiques et les potentielles sanctions financières qui peuvent aller jusqu'à 4% du chiffre d'affaires annuel mondial pour les entreprises qui ne respecteraient pas les normes de confidentialité en vigueur vis-à-vis des internautes situés en Europe.

Retraits du marché européen

Certaines entreprises de presse américaines, qui ont l'habitude de traiter une vaste quantité de données à des fins publicitaires et commerciales, ont donc décidé de se retirer du marché européen de peur de voir leur modèle d'affaires réprimé.

Ces cas anecdotiques ont le mérite de nous rappeler que la gratuité n'existe nulle part. Pas plus que pour le numérique où l'abondance et l'accessibilité des services de l'information ont longtemps entretenu chez les consommateurs l'illusion d'une absence totale de contreparties pour accéder aux innombrables services offerts par le web. La production d'informations a un coût et son commerce a donc un prix. Si ce dernier ne s'exprime pas toujours en unités monétaires pour le consommateur, c'est donc que les concessions portent sur autre chose.

Pour de nombreux opérateurs, cet « autre chose » n'est ni plus ni moins que l'accès et le traitement des données personnelles de leurs clients, souvent à des fins commerciales et publicitaires. Pour s'en convaincre, il suffit de constater que des

entreprises comme Facebook et Twitter refusent l'accès à leurs plateformes respectives à tout utilisateur qui n'accepterait pas de payer le prix demandé, par exemple en restreignant l'usage des *cookies* à l'aide des fonctionnalités présentes sur un navigateur internet.

Le problème du « juste prix »

Toute la vanité du législateur européen à l'origine des nouvelles restrictions réside dans la croyance qu'il peut deviner le « juste prix » des prestations numériques en déterminant de manière centralisée le niveau acceptable de confidentialité pour l'ensemble des utilisateurs d'un service donné.

Or comme nous le relevons à l'IREF dans notre dernier rapport, il n'existe pas de critère objectif pour fixer le degré de confidentialité désirable pour tout le monde. Ce degré dépend de l'expérience intime de l'utilisateur avec son opérateur, du type de données collectées ainsi que la contrepartie attendue à la fourniture de ses informations personnelles. Interférer de manière autoritaire avec ce prix ne peut donc que générer des effets pervers.

De la même façon qu'un contrôle des loyers arbitrairement appliqué affecte la rentabilité des investissements locatifs et les incitations à louer, le contrôle politique du niveau de confidentialité que les entreprises offrent à leurs clients réduit les revenus de l'industrie numérique, dont celle de la publicité ciblée. Tout ceci contribue à raréfier l'offre de services informatiques. Comme toujours, le consommateur est le grand perdant des réglementations qui affectent le commerce. Quand bien même il serait prêt à faire de larges concessions sur ses données personnelles, on ne lui laisse plus le choix.

Le mythe des pleins-pouvoirs de l'entreprise

« Tant mieux », rétorquent les opposants à ces pratiques, pour qui l'usage des données personnelles s'apparente à une dérive du capitalisme numérique et une forme de prédation 2.0. Les industries spécialisées dans le traitement des données personnelles sont accusées d'exploiter l'ignorance et la faiblesse des consommateurs à travers des méthodes cyniques.

La publicité ciblée concentre à elle seule tous les ressentiments, comme si elle donnait aux entreprises les pleins-pouvoirs sur leurs clients, alors qu'elle n'a pas la capacité à se substituer à la qualité des produits fournis. L'irruption publicitaire et la perte de vie privée liées au traitement des données personnelles représentent certes un coût pour le consommateur. Mais ce coût n'est rien à côté des bénéfices que les utilisateurs tirent de l'usage des services financés par les données et la publicité.

Une étude menée en 2010 par le cabinet McKinsey & Compagny constatait que plus de 80% des utilisateurs valorisent beaucoup plus les services offerts par internet que les concessions faites en matière de vie privée et de publicité.

Cette étude constatait que pour chaque euro que l'utilisateur moyen est prêt à dépenser pour limiter les désagréments liés à la perte de vie privée et à la publicité, il évalue à 6 euros les bénéfices qu'il reçoit pour l'usage des applications web financées par la publicité. Grâce à l'enrichissement des contenus disponibles sur le web depuis 2010, on peut légitimement supposer que l'écart entre les concessions et les bénéfices s'est creusé au bénéfice de l'utilisateur. Ceci explique la résilience d'un réseau social comme Facebook.

Un processus où tout le monde est gagnant

Le fait que le « scandale » Cambridge Analytica n'a pas entraîné une hémorragie de ses utilisateurs montre que les bénéfices que ces derniers tirent de l'usage de cette plateforme surpasse les concessions qui consistent par exemple à faire l'objet de campagnes marketing, y compris à des fins politiques. Enfin les critiques de la publicité ciblée négligent son rôle fondamental pour optimiser la rencontre entre les offreurs et les demandeurs de biens et services. Le traitement des données personnelles à des fins publicitaires permet en effet de réduire les coûts des campagnes marketing des entreprises. Les coûts de recherche des entreprises et des consommateurs sont ainsi optimisés. La probabilité que l'utilisateur découvre des produits qui lui sont utiles est augmentée. Toutes les parties prenantes sortent gagnantes de ce processus.

Bien sûr, ce plaidoyer en faveur des services de l'information ne méconnaît pas l'existence de préoccupations légitimes en matière de confidentialité chez les internautes. Le droit pour chaque individu de chercher à restreindre la diffusion de certaines informations jugées sensibles est légitimes. Les clauses de confidentialité sont d'ailleurs monnaie courante dans la vie civile et commerciale. C'est précisément l'une des raisons pour lesquelles la valeur ajoutée d'une réglementation aussi contraignante que le RGPD ou la future législation E-Privacy est faible.

L'utilisateur comme arbitre

De nos jours, il existe déjà sur le marché de nombreuses solutions qui s'adressent aux utilisateurs peu enclins à délivrer leurs données personnelles. Pour les moteurs de recherche, quiconque aspire à plus de confidentialité peut se tourner vers des outils comme DuckDuckGo, Qwant ou Startpage. Pour les services de messagerie électroniques, les applications comme Protonmail ou Telegram sont réputées offrir plus de confidentialité que leurs concurrents respectifs.

Il appartient donc à l'utilisateur d'arbitrer entre les nombreux services proposés en fonction de la vie privée qu'il souhaite concéder. En imposant de strictes normes de confidentialité à l'ensemble des acteurs de l'économie numérique, le législateur génère des coûts inutiles pour les entreprises qui opèrent sur des marchés où la demande de confidentialité est faible ou inexistante.

Il ne faut pas se tromper. L'une des raisons pour lesquelles les revenus générés par l'économie des données aux États-Unis sont deux fois supérieurs au chiffre d'affaires de l'industrie européenne des données est précisément la souplesse de l'environnement juridique américain. Plus respectueux de la subsidiarité, ce dernier associe des règlementations sectorielles souples qui coexistent avec une très forte culture de l'autorégulation. À l'heure où l'Europe ne cesse de de se plaindre de la position dominante des GAFAM et du retard qu'elle prend sur les technologies du future comme l'intelligence artificielle, elle serait mal avisée de rendre la concurrence des nouveaux entrants plus difficiles en érigeant davantage de barrières à l'entrée sur son sol.

Ainsi, si l'unification du marché numérique par l'interdiction pour les États-membres d'ériger des barrières nationales à la circulation des données est l'une des rares bonnes mesures du RGPD, elle risque d'être neutralisée par les autres normes pénalisantes qui côtoient les quelques dispositions libérales. Ceci est d'autant plus vrai que le vocabulaire du Règlement est flou, laissant aux régulateurs un incroyable pouvoir de discrétion et d'interprétation concernant les obligations qui incombent aux entreprises. À défaut de certitudes sur le plan législatif, il incombe dans ces conditions aux observateurs de suivre de près la jurisprudence abondante amenée à se développer.

Le principe de subsidiarité

La solution idéale serait néanmoins de favoriser une régulation plus respectueuse du principe de subsidiarité pour qu'elle corresponde aux mieux aux intérêts de chacun. C'est pourquoi nous proposons de substituer une approche contractuelle aux réglementations infantilisantes. Les normes de confidentialité devraient perdre leur caractère impératif. Les organisations devraient être libres d'adhérer aux standards de leur choix en fonction des préférences de leur clientèle.

Cette approche contractuelle impliquerait de revoir le rôle des autorités administratives indépendantes comme la CNIL. Ces autorités pourraient devenir des tiers de confiance de droit commun chargés d'auditer les politiques de confidentialité des organisations qui éprouveraient le besoin de se soumettre à un examen extérieur pour inspirer confiance auprès de leurs utilisateurs.

Le label European Privacy Seal (EuroPrise) est un exemple parmi d'autres de solutions existantes pour réduire les asymétries d'information lorsqu'il existe une véritable

demande de transparence des processus de traitement. Ces solutions pourraient facilement se généraliser pour peu qu'une véritable concurrence des normes de confidentialité soient restaurée et acceptée par l'opinion publique.